Legislative Audit Division

State of Montana

Report to the Legislature

December 1996 **EDP Audit Report**

Department of Revenue

This report provides information regarding general and application controls over computer data processing systems at the Department of Revenue. It includes recommendations for improving controls within the electronic data processing environment. The recommendations address:

- General and application controls applicable to the department's Computer Assisted Mass Appraisal System (CAMAS).

- Application controls over data processed by the department's Revenue Control System, Delinquent Accounts Receivable, and Individual Income Tax applications.

- Electronic access to CAMAS. This audit determined employees changed personal property information for properties the employees own, which violates department policy.

Direct comments/inquiries to:
Legislative Audit Division
Room 135, State Capitol
PO Box 201705
97DP-04   Helena MT 59620-1705

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Legislative Audit Division are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the division. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MONTANA LEGISLATIVE BRANCH

Legislative Auditor
Scott A. Seacat

Legal Counsel:
John Northey

Deputy Legislative Auditors:
Mary Bryson
Operations and EDP Audit
James Gillett
Financial-Compliance Audit
Jim Pellegrini
Performance Audit

LEGISLATIVE AUDIT DIVISION

December 1996

The Legislative Audit Committee
of the Montana State Legislature:

This report is our EDP audit of general and application controls relating to the Department of Revenue. The audit reviewed general and application controls applicable to the department's Computer Assisted Mass Appraisal System (CAMAS). The audit also addressed application controls over the department's Revenue Control System (RCS), Individual Income Tax System (IIT), and Delinquent Accounts Receivable System (DAR). This report contains recommendations for improving general controls within the CAMAS processing environment. Recommendations also address processing controls over RCS, IIT, and DAR. Written responses to our audit recommendations are included in the back of the audit report.

We thank the Department of Revenue for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

Department of Revenue

Table of Contents

Table of Contents

Table of Contents

Appointed and Administrative Officials

Department of Revenue   Michael Robinson, Director

Judy Paynter, Deputy Director

Dave Woodgerd, Chief Legal Counsel

Judy Jones, Administrator, Operations Division

Jeff Miller, Administrator, Income and Miscellaneous Tax Division

Gary Blewett, Administrator, Liquor Division

Mary Whittinghill, Administrator, Property Assessment Division

Don Hoffman, Bureau Chief, Natural Resource Tax Bureau

Lynn Chenoweth, Bureau Chief, Corporation Tax Bureau

Introduction

This audit reviewed general and application controls at the Department of Revenue. The audit reviewed general controls over the department's AS/400 computer which processes property tax data for the Computer Assisted Mass Appraisal System (CAMAS). Application controls were evaluated for CAMAS, Revenue Control System (RCS), Delinquent Accounts Receivable System (DAR), and Individual Income Tax System (IIT).

A discussion of the audit scope and objectives is included in Chapter I. Further detail for the audit issues summarized below is included in Chapters II through V of the report. *Overall, the audit determined the RCS, DAR, IIT and CAMAS applications process data as intended.*

Revenue Control System

RCS is an automated data recording system and tracks all cash receipts from arrival in the Cashiering Section to posting in a tax processing or collection system. RCS facilitates the recording of revenue collections to the appropriate tax type, timely deposits of cash receipts, and provides automated recording of Statewide Budgeting and Accounting System (SBAS) accounting transactions. RCS processed $1,061 million in tax collections during fiscal year 1996.

Although RCS checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered into RCS is complete and accurate, processed as intended, and posted to department tax systems.*

Delinquent Accounts Receivable

DAR is an automated receivables and collections system. DAR receives and shares information with the major tax processing systems (IIT, Withholding/Payroll Tax, Accommodations Tax, and the Revenue Control System). The system records the collection of debts for all taxes administered by the department. DAR automatically generates notices requesting or demanding payment. Additional automated collection procedures include warrants of

distraint, and levies on employee wages and individual bank accounts. Debts, if not collected through these measures, are automatically assigned to the Warrant Writer Debt Collection Unit at the Department of Administration for further collection action. As of October 31, 1996, the department reported 83,602 receivable accounts on DAR, with a balance of approximately $55 million.

Although DAR checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and posted to receivable accounts.*

Individual Income Tax System

The department's IIT system captures and processes individual income tax returns for the state of Montana, allowing update of name, address, and income data. The system provides batch entry and on-line update of all tax returns and provides up to five years data available through online inquiry.

IIT tracks moneys sent to the department and provides for posting and maintenance of payments in the RCS. IIT automatically generates the appropriate SBAS transactions when moneys are transferred or adjusted and generates warrant transactions for income tax refunds. The system also posts, tracks, and adjusts tax accounts when payments are late or insufficient. As of October 31, 1996 the department recorded 425,016 income tax returns filed for tax year 1995.

Although IIT checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and updated to DAR.*

Processing Edits Should be Documented

Industry guidelines suggest management document limit and reasonableness checks incorporated within programs. The audit determined the department should document existing system edits to ensure personnel are aware of processing decisions performed by the IIT system. Department programmers generated a report of system edits but employees responsible for processing tax returns did not provide accurate definitions of the edit functions.

Based on the edit definitions provided and audit results, employees do not have an accurate understanding of the edit processing decisions. Unless documented, personnel may not make informed decisions regarding selective audit procedures.

Income Tax Return Adjustments Should be Supported

The department's Office Audit Bureau employees review income tax returns which fail processing checks performed by the IIT system. Error conditions may include mathematical computations which disagree with IIT calculations. Department procedures provide that employees document why they clear edit error conditions or make adjustments to tax returns. Employees may also override warning edits at their discretion.

One of the 58 income tax returns reviewed included an underpayment penalty of $414 which employees adjusted to zero without supporting documentation. Upon further review, a department employee noted the prior year return included a $500 underpayment penalty which an employee adjusted to zero without supporting documentation. Since we brought this error to the department's attention, employees have begun collection procedures.

Income Tax Tolerance Levels

The IIT system recomputes individual tax returns to determine mathematical accuracy of returns as submitted by taxpayers. The department established a system tolerance level which allows returns with incorrect tax calculations to process without flagging the return for review. If the difference between taxpayer and IIT system calculations exceeds the tolerance level, the system flags the return for employee review and correction. Employees decide whether or not to adjust computation errors if the errors fall within the tolerance limit. The audit results indicate the department should establish

distraint, and levies on employee wages and individual bank accounts. Debts, if not collected through these measures, are automatically assigned to the Warrant Writer Debt Collection Unit at the Department of Administration for further collection action. As of October 31, 1996, the department reported 83,602 receivable accounts on DAR, with a balance of approximately $55 million.

Although DAR checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and posted to receivable accounts.*

Individual Income Tax System

The department's IIT system captures and processes individual income tax returns for the state of Montana, allowing update of name, address, and income data. The system provides batch entry and on-line update of all tax returns and provides up to five years data available through online inquiry.

IIT tracks moneys sent to the department and provides for posting and maintenance of payments in the RCS. IIT automatically generates the appropriate SBAS transactions when moneys are transferred or adjusted and generates warrant transactions for income tax refunds. The system also posts, tracks, and adjusts tax accounts when payments are late or insufficient. As of October 31, 1996 the department recorded 425,016 income tax returns filed for tax year 1995.

Although IIT checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and updated to DAR.*

Processing Edits Should be Documented

Industry guidelines suggest management document limit and reasonableness checks incorporated within programs. The audit determined the department should document existing system edits to ensure personnel are aware of processing decisions performed by the IIT system. Department programmers generated a report of system edits but employees responsible for processing tax returns did not provide accurate definitions of the edit functions.

Based on the edit definitions provided and audit results, employees do not have an accurate understanding of the edit processing decisions. Unless documented, personnel may not make informed decisions regarding selective audit procedures.

Income Tax Return Adjustments Should be Supported

The department's Office Audit Bureau employees review income tax returns which fail processing checks performed by the IIT system. Error conditions may include mathematical computations which disagree with IIT calculations. Department procedures provide that employees document why they clear edit error conditions or make adjustments to tax returns. Employees may also override warning edits at their discretion.

One of the 58 income tax returns reviewed included an underpayment penalty of $414 which employees adjusted to zero without supporting documentation. Upon further review, a department employee noted the prior year return included a $500 underpayment penalty which an employee adjusted to zero without supporting documentation. Since we brought this error to the department's attention, employees have begun collection procedures.

Income Tax Tolerance Levels

The IIT system recomputes individual tax returns to determine mathematical accuracy of returns as submitted by taxpayers. The department established a system tolerance level which allows returns with incorrect tax calculations to process without flagging the return for review. If the difference between taxpayer and IIT system calculations exceeds the tolerance level, the system flags the return for employee review and correction. Employees decide whether or not to adjust computation errors if the errors fall within the tolerance limit. The audit results indicate the department should establish

distraint, and levies on employee wages and individual bank accounts. Debts, if not collected through these measures, are automatically assigned to the Warrant Writer Debt Collection Unit at the Department of Administration for further collection action. As of October 31, 1996, the department reported 83,602 receivable accounts on DAR, with a balance of approximately $55 million.

Although DAR checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and posted to receivable accounts.*

Individual Income Tax System

The department's IIT system captures and processes individual income tax returns for the state of Montana, allowing update of name, address, and income data. The system provides batch entry and on-line update of all tax returns and provides up to five years data available through online inquiry.

IIT tracks moneys sent to the department and provides for posting and maintenance of payments in the RCS. IIT automatically generates the appropriate SBAS transactions when moneys are transferred or adjusted and generates warrant transactions for income tax refunds. The system also posts, tracks, and adjusts tax accounts when payments are late or insufficient. As of October 31, 1996 the department recorded 425,016 income tax returns filed for tax year 1995.

Although IIT checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and updated to DAR.*

Processing Edits Should be Documented	Industry guidelines suggest management document limit and reasonableness checks incorporated within programs. The audit determined the department should document existing system edits to ensure personnel are aware of processing decisions performed by the IIT system. Department programmers generated a report of system edits but employees responsible for processing tax returns did not provide accurate definitions of the edit functions.

Based on the edit definitions provided and audit results, employees do not have an accurate understanding of the edit processing decisions. Unless documented, personnel may not make informed decisions regarding selective audit procedures.

Income Tax Return Adjustments Should be Supported

The department's Office Audit Bureau employees review income tax returns which fail processing checks performed by the IIT system. Error conditions may include mathematical computations which disagree with IIT calculations. Department procedures provide that employees document why they clear edit error conditions or make adjustments to tax returns. Employees may also override warning edits at their discretion.

One of the 58 income tax returns reviewed included an underpayment penalty of $414 which employees adjusted to zero without supporting documentation. Upon further review, a department employee noted the prior year return included a $500 underpayment penalty which an employee adjusted to zero without supporting documentation. Since we brought this error to the department's attention, employees have begun collection procedures.

Income Tax Tolerance Levels

The IIT system recomputes individual tax returns to determine mathematical accuracy of returns as submitted by taxpayers. The department established a system tolerance level which allows returns with incorrect tax calculations to process without flagging the return for review. If the difference between taxpayer and IIT system calculations exceeds the tolerance level, the system flags the return for employee review and correction. Employees decide whether or not to adjust computation errors if the errors fall within the tolerance limit. The audit results indicate the department should establish

procedures to ensure employees consistently adjust tax returns for the tolerance errors.

Industry guidelines suggest management document system processing decisions and functions. Audit results indicate the department has not documented or communicated to employees its policy for correcting tolerance errors during tax return review. Although the department has established a tolerance level to minimize tax return processing costs, the department could not provide supporting documentation for the tolerance level.

CAMAS

The department's CAMAS assists employees in creating and maintaining property valuation data for each county in the state. The database holds the records of property characteristics that affect the tax valuation of each parcel in the state. CAMAS maintains previous, current, and future year information for the current appraisal cycle as well as future reappraisal information. CAMAS programs assist the appraiser in analyzing property data to arrive at a property valuation. Property administration data, such as owner's name, mailing address, legal descriptions, and market and taxable value is entered and maintained on the Montana Ownership Database System (MODS), and is transferred electronically to CAMAS.

General Controls

The audit concluded overall general controls provide controlled application processing for CAMAS. However, the department should complete disaster recovery procedures to ensure continued operation of CAMAS in the event of a disaster. The audit determined the department could improve physical security controls by installing a smoke alarm within the data center and providing secured storage for backup tapes. The department should also evaluate operating system software installation parameters for compliance with industry guidelines. These issues are discussed in Chapter IV.

Application Controls

The audit reviewed a sample of 58 properties located in Blaine, Fergus, Gallatin, Madison and Silver Bow counties to determine if CAMAS provides accurate and reliable processing results. The audit reviewed data entry controls (including electronic access) which ensure data entered is authorized, accurate, complete, and valid. The audit also reviewed processing controls which ensure data entered is processed as intended. We also verified system output controls ensure property valuation data provided to counties is complete and accurate based on system processing results. *The audit concluded input controls over CAMAS should be improved. Processing and output controls ensure data entered is processed as intended and provided to county offices.* The issues summarized below are discussed in Chapter IV beginning on page 25.

Password Security Should be Improved

CAMAS application security software does not allow or force users to select confidential passwords, or periodically change the passwords. The CAMAS security officer assigns user logon IDs and passwords to system users, and documents the assignment in a letter provided to each user. The user is encouraged to keep the password confidential, but is not given the option to periodically change it. We also found passwords may be easily guessed, based on the methods used for password assignment.

Industry guidelines suggest management implement procedures to prevent unauthorized system access. Passwords should be changed at least every 60 days and, if they must be documented, the passwords should be secured from unauthorized access. Unless password controls are improved, unauthorized individuals could access CAMAS and view or change confidential property valuation data.

Electronic Access Should Agree with Employee Job Duties

The department requires regional and county officials to notify the department in writing if an employee needs additional access beyond the default access initially granted. However, once granted, the access levels are not reviewed on a scheduled basis to determine if the access is appropriate based on the employee's current job duties. For instance, an employee may only require temporary access, or may change job duties. The audit identified several employees with unnecessary access to CAMAS.

Industry guidelines suggest management implement controls to ensure user access agrees with employee job duties. The department believes employee responsibilities may have changed since the employees were first assigned access to CAMAS. Based on the testing performed, the department should confirm access granted with the employees' supervisor, periodically review access granted, and restrict employee access in accordance with job duties.

Changes to Employee-Owned Property Against Department Policy

Regional managers are requested to review employee-owned properties at least once every appraisal cycle, to ensure compliance with department policy. Department policy prohibits employees from appraising or making system changes to property they own, or property owned by family members.

Of 54 department employees reviewed, the audit identified 36 employees who own real property recorded on CAMAS. The audit determined 18 of the 36 employees entered changes to the properties they owned, based on our review of the CAMAS audit trail report. We identified changes to property characteristics which caused changes to the taxable valuation for some of the properties reviewed. Based on audit results, the department should implement additional management controls to restrict employees from making changes to their properties on CAMAS.

Internal Audit Follow-up Procedures Should be Established

The department's Property Assessment Division performs internal audits of CAMAS appraisal/assessment staff procedures. Internal audits address property valuation procedures and methodologies as implemented by employees according to department policy. The internal audit employees issue reports of their findings and recommendations to the counties, regions, and management staff. However, the department does not review the status of the audit recommendations to ensure the recommendations are implemented. Instead, the department requests county and regional staff implement the recommendations.

Without department follow-up, internal audit recommendations may not be implemented. We believe the department should establish implementation deadlines and perform follow-up reviews to ensure the recommendations are implemented. The department could

request county offices to report the implementation status for recommendations issued by the department.

Department-wide Issues

Chapter V discusses electronic access controls specific to RCS, DAR and IIT. In addition, the chapter provides recommendations concerning disaster recovery and security evaluations over information technology resources. The issues summarized below are discussed in Chapter V on page 33.

Electronic Access Issues - RCS, DAR and IIT

The audit identified employees have unnecessary update access to RCS, DAR and IIT application programs and/or data. Update access allows employees to add or change data included on income tax returns such as income, withholding, exemptions, and deductions. Update access also allows employees to correct processing errors identified by system edits or override the edit errors. Access to RCS and DAR could allow unauthorized changes to revenue collection data or outstanding tax receivable balances, respectively. The audit also found employee access was documented for some but not all employees, on authorized request forms.

Programmer write access to production programs and data should be restricted, logged and monitored. Documented and properly authorized access requests help management maintain security over system data. The department should limit employee access to application data in accordance with job duties. Unnecessary access privileges compromise the integrity of data processed by the RCS, DAR, and IIT applications.

Disaster Recovery Plans Should be Completed

Industry standards suggest management develop formal procedures to efficiently recover computer processing activities to normal operations following a disaster. The Montana Operations Manual section 1-0240.00 outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing information and resource requirements necessary to maintain applications; and determining alternate procedures which may be necessary if recovery cannot be completed timely.

The department has not completed a formal disaster recovery plan to return department applications to normal operations following a

disaster. An effective disaster recovery plan should allow management to restore computing operations in a set time and minimize losses. Without a complete disaster recovery plan which defines department responsibilities and requirements, the department may be unable to process its applications.

Chapter I - Introduction and Background

Introduction

This is an electronic data processing audit of general and application controls at the Department of Revenue. The audit reviewed general controls over the department's AS/400 computer which processes property tax data for the Computer Assisted Mass Appraisal System (CAMAS). The audit also evaluated application controls over CAMAS, Revenue Control System (RCS), Delinquent Accounts Receivable System (DAR), and Individual Income Tax System (IIT). Except for CAMAS, the systems noted above process data on the Department of Administration's central mainframe computer.

Organization of Report

The report is organized into five chapters. Chapter I provides an introduction, background information, and audit objectives. Chapters II and III discuss application controls and audit recommendations for RCS, DAR, and IIT. Chapter IV includes the review of general and application controls over CAMAS and related audit recommendations. Chapter V discusses department-wide issues based on overall audit findings.

General and Application Controls

EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed.

A general control review provides information about the environment in which applications process data and includes an examination of the following controls:

Organizational - apply to the structure and management of the computing and information services facility. Specific types of organizational controls include segregation of duties, assignment of responsibilities, rotation of duties, and supervision.

Procedural - operating standards and procedures which ensure the reliability of computer processing results and protect against processing errors.

Hardware and Software - controls within the operating system software and hardware which monitor and report system error conditions.

System Development - oversight and supervisory controls imposed on development projects. Controls include feasibility studies, development, testing and implementation, documentation, and maintenance.

Physical Security - physical site controls including security over access to the computer facility, protection devices such as smoke alarms and sprinkler systems, and disaster prevention and recovery plans.

Electronic Access - controls which allow or disallow user access to electronically stored information such as data files and application programs.

Application controls are specific to a given application or set of programs that accomplish a specific function. The review includes an examination of the following controls and objectives.

Input - Ensure all data is properly coded to machine language, all entered data is approved, and all approved data is entered.

Processing - Ensure all data input is processed as intended.

Output - All processed data is reported and properly distributed to authorized individuals. Output may include hard copy reports, or electronic data reported online or shared with other computer applications.

A review of the application documentation and audit trail is also performed. Applications must operate within the general control environment in order for reliance to be placed on them. General controls over applications which process data at the Department of Administration's mainframe computer center are evaluated during the annual audit "Information Processing Facility and Central Applications." (96DP-06)

Audit Objectives

The objectives of this audit were to evaluate the:

1. General controls specific to the department's mid-level data processing center which processes CAMAS application data. The audit reviewed the department's data processing center operations and procedures which support CAMAS application processing functions.

2. Application controls over data processed by the RCS, DAR,
    IIT, and CAMAS applications. The audit also included an
    evaluation of the interface (sharing of information) between
    RCS, DAR, and IIT.

**Audit Scope and
Methodology**

The audit was conducted in accordance with government audit
standards. We compared the department's general and application
controls against criteria established by the American Institute of
Certified Public Accountants (AICPA), United States General
Accounting Office (GAO), and the information technology industry.

The audit reviewed the department's general controls related to the
mid-level computer environment. For example, we interviewed
department personnel to gain an understanding of the hardware and
software environment, and examined documentation to supplement
and confirm information obtained through interviews. We also
evaluated procedures which ensure CAMAS processing activities are
controlled by reviewing equipment maintenance procedures and
physical access to processing areas. We reviewed department
procedures which ensure data processing for RCS, DAR, IIT, and
CAMAS is completed according to user authorization.

The audit reviewed the department's application controls related to
RCS, DAR, IIT, and CAMAS. We evaluated employee policies and
procedures, and reviewed input, processing, and output controls for
these systems. For example, we reviewed data entry and processing
over income tax returns by testing input edits and evaluating
processing results. We verified IIT performs accurate mathematical
review of tax return data. We also traced related tax return data
through RCS and DAR to ensure all systems include complete and
accurate information. We also reviewed supporting documentation
to determine if controls over data are effective as well as adequate to
ensure the accuracy of data during processing phases.

Chapter I - Introduction and Background

Compliance

The audit reviewed application processing for compliance with state law. We ensured individual income taxes, and related interest and penalties are processed according to state law. The audit also reviewed the department's compliance with existing department data processing procedures and policy. We also reviewed electronic access controls which ensure department compliance for access to confidential information.

Department Background

The Department of Revenue was created by the Executive Reorganization Act of 1971 to administer state tax laws. The department currently consists of the Director's Office and five divisions. The duties and functions of the office and divisions are described as follows:

▸ The Director's Office is responsible for advising the Governor on matters affecting the department, recommending changes to Montana tax laws and policies, providing policy direction to all divisions within the department, and coordinating the department's biennial budget. The Offices of Legal Affairs, Investigation, Research and Information, and Personnel and Training are part of the Director's Office.

▸ The Income and Miscellaneous Tax Division administers the Individual Income Tax System and Montana individual income tax laws, including employer withholding and the Workers' Compensation Old Fund Liability Tax. The division also administers miscellaneous taxes and licenses not administered by other divisions including tobacco, accommodations, inheritance, and estate taxes.

▸ The Liquor Division is responsible for administering the state alcoholic beverage codes, including taxation, licensure, and regulation. It also supervises the operation of the liquor enterprise activities consisting of a liquor warehouse and agency liquor stores.

▸ The Natural Resource and Corporation Tax Division is responsible for administering taxes, including corporation license tax; coal, oil, gas, and local government severance taxes; gross and net proceeds taxes; metal mines tax; electrical energy license tax; and resource indemnity trust tax. The division also is responsible for administering the state and federal royalty audit programs related to mineral production on state and federal lands located in Montana.

- The Property Assessment Division administers the CAMAS application and is responsible for valuing all taxable property in the state. The division is charged with securing a fair, uniform, and equitable valuation of all taxable property within and among counties, between different classes of property, and between individual taxpayers.

- The Operations Division administers RCS and DAR. The division also provides automated word and data processing services, detailed systems requirements analysis, systems development and maintenance services, data entry services, computer operations support services, technical support, and research services for the department. The division also provides support services, including central mail processing, cashiering, accounting, and payroll.

The department uses several different computer applications in its daily operations. The audit concentrated on four applications and reviewed computer processing activities in three divisions. We reviewed application controls applicable to the Individual Income Tax System, Revenue Control System, and Delinquent Accounts Receivable System, as operated by the Income and Miscellaneous Tax Division. The audit also reviewed application controls over the CAMAS application as operated by the Property Assessment Division. General controls over CAMAS, as operated by the Operations Division were also reviewed.

The department is evaluating replacing the IIT, DAR and CAMAS systems with newer technology. Recommendations included in this report address changes to existing department procedures and system processing functions. To implement the recommendations, we recognize the department must modify existing systems or develop solutions within replacement systems. Where possible, we have provided the department with alternative procedures for implementing the recommendations.

Chapter II - Revenue Control and Delinquent Accounts Receivable Systems

Revenue Control System

The department processes approximately 800,000 revenue collection transactions a year. The department uses the RCS to track revenue collections for all taxes administered by the department. RCS is an automated data recording system and tracks all cash receipts from arrival in the Cashiering Section to posting in a tax processing or collection system. All automated tax processing or collection systems electronically transfer information to and from RCS to reconcile payments as they update tax accounts. With non-automated systems, employees manually reconcile RCS collections to the various tax systems.

RCS facilitates the recording of revenue collections to the appropriate tax type. RCS processed $1,061 million in tax collections during fiscal year 1996. RCS also facilitates timely depositing of revenues to the state treasury and provides automated recording of Statewide Budgeting and Accounting System (SBAS) accounting transactions. At the close of each day, collection reports are produced and sent to the State Treasurer. Daily transactions are updated to SBAS and reconciled to ensure a complete and accurate transfer.

Conclusions Over RCS

The audit reviewed data entry procedures which ensure revenue collections are completely and accurately entered to RCS. The audit also reviewed employee procedures which ensure revenue collections recorded in RCS are posted to the appropriate tax account. For example, we verified individual income tax receipts recorded in RCS were accurately posted to the Individual Income Tax System. We also evaluated employee procedures for reconciling data entry between RCS and the department tax systems.

Although RCS checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed further in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered into RCS is complete and accurate, processed as intended, and posted to department tax systems.*

Delinquent Accounts Receivable

DAR is an automated receivables and collections system. DAR receives and shares information with the major tax processing systems (IIT, Withholding/Payroll Tax, Accommodations Tax, and the Revenue Control System). As of October 31, 1996, the department reported 83,602 receivable accounts on DAR, with a balance of approximately $55 million. The system records the collection of debts for all taxes administered by the department.

Receivables are entered into DAR either manually or automatically by a tax processing system through the department's Accounts Receivable Inter-System Interface (ISI) process. Adjustments and payments are applied either via an on-line session or ISI.

DAR automatically generates notices requesting or demanding payment. Additional automated collection procedures include warrants of distraint, and levies on employee wages and individual bank accounts. Debts, if not collected through these measures, are automatically assigned to the Warrant Writer Debt Collection Unit at the Department of Administration for further collection action.

Conclusions Over DAR

The audit reviewed manual and automated data entry procedures which ensure receivables are updated completely and accurately entered to DAR. The audit also reviewed employees' use of DAR to collect account receivables established by the IIT. We verified IIT account balances due are completely and accurately posted to DAR. The audit also evaluated employee collection procedures and electronic access to DAR. The audit reviewed processing and output controls which ensure penalty and interest assessments for tax due are accurately posted to receivable accounts.

Although DAR checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed further in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and posted to receivable accounts.*

The audit reviewed information updated to DAR from the IIT system and identified a concern which may reduce employee productivity. The issue is discussed below.

**Case Notes Should be
Updated for Address
Changes**

DAR employees record case notes within the system which provide collection history data for each delinquent account. Case notes include prior taxpayer addresses, documentation of correspondence with taxpayers, and collection actions taken. Based on contact with the taxpayer, DAR employees may update the taxpayer's address. DAR automatically posts the prior address to the case notes to maintain an accurate case history.

Industry guidelines suggest management implement controls to provide a complete audit trail of transactions. The IIT system updates DAR with taxpayer addresses submitted on tax forms, but does not update DAR case notes with the prior address. As a result, DAR employees must research income tax files or microfiche reports, or contact the taxpayer for prior address information.

The department has requested Operations Division programming staff establish a universal note screen that can be shared by department systems. A universal note screen could allow centralized case note update for taxpayer accounts without over-writing existing address data. However, the department has placed this system modification request at a low priority. As an alternative, the department could direct employees to record current address information within the DAR case notes.

Recommendation #1

We recommend the department evaluate system procedures to ensure IIT address changes do not over-write existing DAR address data.

Chapter III - Individual Income Tax System

The department's IIT system captures and processes individual income tax returns for the state of Montana, allowing update of name, address, and income data. The system provides batch entry and on-line update of all returns (long and short form, fiduciary, elderly homeowner/renter credit, partnership, back year, and amended). The system provides up to five years data available through online inquiry.

IIT tracks moneys sent to the department and provides for posting and maintenance of payments in the RCS. IIT automatically generates the appropriate SBAS transactions when moneys are transferred or adjusted and generates warrant transactions for income tax refunds. The system also posts, tracks, and adjusts tax accounts when payments are late or insufficient. DAR facilitates collection of moneys owed by assessing various penalties and interest, and by generating delinquency and collection notices.

The audit reviewed individual income tax returns processed through IIT for the 1995 tax year as follows:

- Form 2 - Long Form. Required for taxpayers who met one of the following criteria.

  -- Montana resident for only part of the tax year.

  -- Nonresident with income from Montana sources.

  -- Married, filing separate returns.

  -- Use an itemized deduction schedule.

  -- Income sources included business or profession, rents, royalties, partnerships, trust or S corporation, capital gain(s).

  -- Or claiming tax credits.

- Form 2S - Short Form. Taxpayers could file this form if they met the following criteria.

  -- Montana resident during the entire tax year.

-- Filing from a Montana address.

-- Filing status was single, head of household, or married filing a joint return.

-- Deductions limited to the standard deduction or federal income tax paid or withheld.

-- Tax credit limited to Elderly Homeowner/Renter Credit.

-- Income sources were limited to wages, pensions and annuities, interest and dividends, fees, alimony, unemployment, winnings, prizes, awards, or other miscellaneous income.

Electronic Filing

Beginning in January 1995, the department accepted electronically filed income tax returns from resident tax filers. This automated process allowed tax filers to file Form 2 and Form 2S tax returns electronically through an authorized processor using a personal computer. The data was transmitted electronically to the Internal Revenue Service and later retrieved by the department and loaded to the IIT system. To ensure authenticity and accuracy, the tax filers were required to submit Form 8453 - Declaration for Electronic Filing, to the department. Employees processed the data through IIT for mathematical accuracy and error resolution.

Conclusions Over IIT

The audit reviewed a representative statistical sample of 407,376 1995 individual income tax returns filed as of September 25, 1996. We evaluated department procedures for processing tax returns by reviewing data entry controls, application processing functions, and controls over system output such as issuing refunds or assessing additional tax. The audit reviewed income tax returns for accuracy of data entry, supporting documentation, mathematical accuracy, and accuracy of refunds or additional tax assessments. The audit also evaluated the interface with DAR.

The audit also reviewed a representative statistical sample of 11,489 returns filed electronically for the 1995 tax year. The audit objective was to ensure returns filed electronically were supported by the tax form submitted directly to the department by the tax filer. Audit procedures verified the electronic returns agreed with and

were supported by the tax filers' form submitted directly to the department.

Although IIT checks data entry for completeness and validity, the lack of adequate electronic access controls could allow unauthorized users to access and change system data. This issue is discussed further in Chapter V. *Except for electronic access concerns, the audit concluded application controls ensure data entered is complete and accurate, processed as intended, and updated to DAR.* The following sections discuss the review and recommendations where the department could improve input, processing and output controls associated with the IIT application.

System Edits

System edits check data input for validity, accuracy, format, and reasonableness. Edits may range from simple checks of an input field length, to verifying input data against calculations or preexisting data already recorded in the computer system. The audit reviewed system edits which check data entry for completeness and accuracy and inspect data for compliance with expected processing results. For example, the audit reviewed data input edits which compare information entered from a tax return to expected values. The audit also reviewed processing edits which ensure mathematical accuracy of tax return calculations.

System edits ensure data entry agrees to the information provided on the taxpayer return. Processing edit checks evaluate the data entered and flag returns which include incomplete or inaccurate information. For example, tax returns with head of household filing status are checked to ensure dependents are included as exemptions. Tax returns flagged for review are reported to the department's Office Audit Bureau for examination. Office Audit Bureau employees resolve the errors and then release the returns to complete system processing.

The issues below identify our concerns regarding system processing edits and provide recommendations where the department could improve processing procedures.

Processing Edits Should be Documented

The audit reviewed system edits by entering and processing test returns through the IIT system. Edit documentation was not readily available. Department programmers generated a report of system edits following our request for the information, but employees responsible for processing tax returns did not provide accurate definitions of the edit functions. After we obtained the department's representation of IIT system edits, audit tests were completed to ensure the edits check data as intended. Based on the edit definitions provided and audit results, employees do not have an accurate understanding of the edit processing decisions. In addition, the edit listing provided by department programmers was not complete.

The audit identified system edits that did not test for data accuracy or identify tax returns for further review as intended. The following are examples where department personnel believed these edits existed in the system and relied upon the edits to flag returns for further review or processing. After we completed the audit, department management clarified their understanding of the system edits.

- Tax law allows charitable contribution deductions between 20 percent to 50 percent of adjusted gross income, depending on the type of contribution or recipient. An edit intended to check for contributions greater than $100,000 failed to identify deductions that exceeded that amount.

- An edit management believed to identify property tax deductions on Form 2A that are greater than $20,000 failed to flag such deductions. This edit accurately tests the deduction on the Elderly Homeowner/Renter Credit form.

- An edit management believed to identify a taxable income reduction for unemployment income greater than $50,000 failed to flag such reductions. The taxable income reduction is allowed on Form 2 and 2S.

In addition to review of error conditions during initial processing, Office Audit Bureau employees perform selective audits on tax returns that meet specific criteria. For example, the department recently reviewed tax returns with adjusted gross income greater than $100,000 and no tax liability. However, the department has

not performed a selective audit on returns with charitable contributions or property tax deductions because personnel believed edits identified the returns for review and correction during initial processing.

Industry guidelines suggest management document limit and reasonableness checks incorporated within programs. The audit issues indicate the department should document existing system edits to ensure personnel are aware of processing decisions performed by the IIT system. Unless documented, personnel may not make informed decisions regarding selective audit procedures.

Recommendation #2

We recommend the department document Individual Income Tax system edits for management and personnel review.

Income Tax Return Adjustments Should be Supported

The department's Office Audit Bureau employees review income tax returns which fail processing checks performed by the IIT system. For example, edits check for math accuracy by recalculating tax due. Error conditions may include mathematical computations which disagree with IIT calculations. Bureau employees evaluate the error conditions and clear errors to complete return processing. Department procedures provide that employees document why they clear edit error conditions or make adjustments to tax returns.

One of the 58 income tax returns reviewed included an underpayment penalty of $414 which employees adjusted to zero without supporting documentation. Upon further review, a department employee noted the prior year return included a $500 underpayment penalty which an employee adjusted to zero without supporting documentation. Since we brought this error to the department's attention, employees have begun collection procedures.

The IIT system allows employees to override warning edits based on the employees' discretion. For example, employees may override a warning edit that identifies tax returns which claim taxes withheld in

excess of set limits. Because all employees can override this warning, the tax returns may be processed without correction.

The IIT system can produce a log of adjustments and error overrides completed by Office Audit Bureau employees. The log identifies total returns processed per employee, adjustments completed, and warning edits overridden. To ensure adjustments are properly supported and authorized, management could periodically review employee transactions documented in the log.

Recommendation #3

We recommend the department establish procedures for periodic review of processing edit adjustments completed by Office Audit Bureau employees.

Income Tax Tolerance Levels

The IIT system recomputes individual tax returns to determine mathematical accuracy of returns as submitted by taxpayers. The department established a system tolerance level which allows returns with incorrect tax calculations to process without flagging the return for review. If the difference between taxpayer and IIT system calculations exceeds the tolerance level, the system flags the return for employee review and correction. In addition, if returns are flagged for review due to other error conditions, department personnel noted employees correct mathematical errors identified within the tolerance limit.

We reviewed a representative statistical sample of individual income tax returns with adjustments made by employees. The audit objective was to ensure employees correct mathematical errors on tax returns flagged for employee review. Although department personnel believe the employees correct all tolerance errors during review, we found computation errors which employees did not correct. Management explained they have established a limit within the tolerance limit. This limit is based on the additional processing and administrative cost of correcting the error.

Industry guidelines suggest management document system processing decisions and functions. Audit results indicate the department has not documented or communicated to employees its policy for correcting tolerance errors during tax return review. Although the department has established a tolerance level to minimize tax return processing costs, the department could not provide supporting documentation for the tolerance level.

Currently, employees decide whether or not to adjust computation errors if the errors fall within the tolerance limit. The audit results indicate the department should establish procedures to ensure employees consistently adjust tax returns for the tolerance errors.

Recommendation #4

We recommend the department document and communicate its policy for adjusting tolerance errors and implement procedures to ensure compliance with the policy.

Chapter IV - Computer Assisted Mass Appraisal System

Introduction

The department's CAMAS assists employees in creating and maintaining property valuation data for each county in the state. The database holds the records of property characteristics that affect the tax valuation of each parcel in the state. CAMAS maintains previous, current, and future year information for the current appraisal cycle as well as future reappraisal information.

CAMAS is designed to build and maintain consistent and accurate computerized files of property data (land and improvements) for residential, agricultural, commercial, and industrial properties. CAMAS produces computer assisted cost and market valuations of the residential and agricultural properties. It also produces cost and income valuations for commercial and industrial properties. CAMAS programs assist the appraiser in analyzing property data to arrive at a property valuation. Property administration data, such as owner's name, mailing address, legal descriptions, and market and taxable value is entered and maintained on the Montana Ownership Database System (MODS), and is transferred electronically to CAMAS. MODS data is stored in a separate subsystem within CAMAS.

The CAMAS system provides the department with three approaches to determine taxable value as described below.

Cost Approach - Provides appraisers the ability to estimate the depreciated cost of reproducing or replacing a building and its site improvements. This is accomplished by determining the replacement cost of a new structure and deducting any loss in value due to physical deterioration, and functional or economic obsolescence. The cost approach can be used for all types of construction on each type of property. It is a starting point for appraisers in determining a property value. The cost approach is most often used where adequate market and/or income data is not available for a particular property or type of property.

Market Approach - Appraisers value property using the comparable sales approach to establish market value. When a sufficient number of sales are available, market models can be developed. The models

are then applied, in conjunction with a comparable sales analysis, to provide an estimate of the market value of each property. In making this analysis, individual properties are valued using three to five comparable sales. The comparable sales are adjusted for differences such as square footage of living area, location, year built, date of sale, quality grade, etc. The adjustments for each comparable are then applied to their sale price. The result is an estimate of value for the subject property, based on the adjusted sales of comparable properties.

Income Approach - Appraisers value income producing properties using the income approach. In applying the income approach to value, the appraiser must determine market rents, expenses and appropriate capitalization rates. The appraiser develops a basic set of income and expense models based on market data. Through use of a capitalization rate, income is capitalized into an estimate of value. The models created reflect current economic trends in specific valuation areas. The value indications produced by the income approach and the cost approach are compared, and a final value for the property is determined.

The primary function of CAMAS is to assist the department in determining uniform, accurate, equitable and defensible valuations of all types of classes of real property statewide. CAMAS operates on the department's AS/400 computer, located in the Mitchell Building. Appraisers in each of Montana's 56 counties input and access information through personal computers connected to the AS/400 through the Department of Administration's mainframe data center.

The audit reviewed general and application controls over CAMAS. We examined procedures within the department's data center which ensure computer processing activities are controlled. We also reviewed application controls to ensure data is processed as intended by CAMAS. The first section of this chapter discusses the general control review. Beginning on page 24 is the discussion of application controls.

General Controls

The department's Operations Division operates the AS/400 computer processing center, located in the Mitchell Building in Helena. Department employees process property tax appraisal data using the CAMAS application programs and data stored on the computer. CAMAS is accessed by employees through personal computers and terminals located in Helena and county offices.

Conclusions Over General Controls

The audit concluded overall general controls provide controlled application processing for CAMAS. However, we determined the department should complete disaster recovery procedures to ensure continued operation of CAMAS in the event of a disaster. The audit determined the department could improve physical security controls by installing a smoke alarm within the data center and providing secured storage for backup tapes. The department should also evaluate operating system software installation parameters for compliance with industry guidelines. These issues are discussed below.

Fire Detection Controls

The audit reviewed existing physical security controls within the data center. We noted the department restricts access to the facility to authorized personnel, and the power supply and temperature within the facility meet computing equipment needs. Although the department maintains a fire extinguisher within easy access, the department has not installed a smoke detector within the facility.

Industry standards suggest management implement cost-effective controls to prevent or limit damage to computer equipment caused by excessive heat or fire. Because employees periodically leave the computer facility unattended, a smoke detector could alert employees of fire or smoke. The cost of a smoke alarm is minimal compared to the cost of extensive damage or loss of computer hardware resulting from a fire.

Recommendation #5

We recommend the department implement cost-effective controls to prevent or limit damage to computer facility equipment.

Off-site Storage of Backup Data

The audit reviewed department procedures which ensure CAMAS software and data are backed up regularly and stored in a secure location to prevent accidental loss. Department employees regularly backup operating system software, and CAMAS programs and data, which they store offsite. However, backup tapes remain in the computer facility until the following day for delivery to the department's Property Assessment Division off-site location. The storage location is not kept locked and employees do not maintain an inventory listing of the tapes stored offsite.

Industry guidelines suggest management store backup copies of system software and application programs and data at a secure off-site location. An inventory of backup tapes should also be maintained for emergency recovery purposes. Unless backup copies are stored in a secure off-site location, the department could lose operating software, application programs and data at the computer facility due to fire.

Employees noted they store the tapes overnight in the computer facility for easier transport to the off-site location the following day. The department could store the tapes in the department's Network Systems section vault overnight. The department could also improve physical access controls at the off-site location or establish an agreement with the Department of Administration, which provides secured off-site storage, including pick-up and delivery, for agency backup data.

Recommendation #6

We recommend the department ensure backup information is stored in a secure off-site location away from the computer facility.

Operating System Software Controls

The department's operating system software includes parameters established during initial installation to control system security. The parameters establish controls over user sign-on attempts, passwords, and operating system configuration. We reviewed the department's operating system software parameters against industry guidelines established for the AS/400 environment. The department installed 12 of 15 parameters differently than suggested by the guidelines. Examples are noted below.

- Guidelines suggest a limit of one logon per user at the same time. The department allows unlimited logon at multiple locations, which increases the risk of unauthorized access to operating system software. The department indicated data operators need to log on to more than one terminal to perform night shift duties.

- Guidelines suggest replacement passwords used to access the operating system software be unique from previously used passwords. Department settings do not require unique replacement passwords.

- Guidelines suggest software-supplied passwords for initial installation logon be changed, since the passwords are common to all AS/400 installations. The passwords allow access to change operating system software parameters. Until our review, the department had not changed the software-supplied passwords.

- The AS/400 Authorized User Roster is not current. The roster identifies user access privileges to the operating system, but several users listed do not require the access.

Industry guidelines suggest management establish security policies for the AS/400 operating system environment. Policies should include procedures to evaluate and document decisions regarding operating system parameters and user privileges. Without such policies, users may make unauthorized changes to the system configuration or application programs and data without detection.

Existing department policy requires each division administrator to appoint a security liaison to develop and implement security procedures. Existing procedures do not specifically address

operating system security. We believe the security procedures should address evaluation and periodic review of the AS/400 operating system security environment.

Recommendation #7

We recommend the department:

A. Evaluate and document AS/400 operating system installation parameters.

B. Develop security procedures over the AS/400 as required by department policy.

Application Controls

The audit reviewed a sample of 58 properties located in Blaine, Fergus, Gallatin, Madison and Silver Bow counties to determine if CAMAS provides accurate and reliable processing results. The audit reviewed data entry controls (including electronic access) which ensure data entered is authorized, accurate, complete, and valid. The audit also reviewed processing controls which ensure data entered is processed as intended. For example, we verified CAMAS computes property valuations accurately based on established processing formulas and sales data. We also verified system output controls ensure property valuation data provided to counties is complete and accurate based on system processing results.

Conclusions Over Application Controls

CAMAS processes data using sale comparisons and cost valuation formulas. The audit reviewed department procedures for maintaining and utilizing the formulas consistently. The audit determined CAMAS processes data as intended and provides reliable results to employees based on data entered. Although CAMAS checks data entry for completeness and validity, electronic access controls do not adequately limit employee access to system data. *The audit concluded input controls over CAMAS should be improved. Processing and output controls ensure data entered is processed as intended and provided to county offices.* Electronic access issues are discussed in the section below.

Electronic Access Controls

Access controls provide electronic safeguards designed to ensure computer system resources are protected from unauthorized use. Access to CAMAS is controlled through three levels of security. Each level requires employees enter a user ID and password. Level one requires employees log on to the department's network. At level two, employees log on to the mainframe computer. Level two provides authorized employees a menu option to select CAMAS. Level three requires employees log on to CAMAS to access the application's main menu.

The following sections discuss the review of employee access to CAMAS (level three). CAMAS application software controls the user's ability to add, modify, delete or view property data. The following sections discuss the audit findings concerning access control over CAMAS and include recommendations to improve overall input controls.

Password Security Should be Improved

CAMAS application security software does not allow or force users to select confidential passwords, or periodically change the passwords. The CAMAS security officer assigns user logon IDs and passwords to system users, and documents the assignment in a letter provided to each user. The user is encouraged to keep the password confidential, but is not given the option to periodically change it. The passwords are also stored in a binder at the security officer's desk and are not secured from unauthorized access, except at night.

The security officer assigns logon IDs and passwords in consecutive order to CAMAS users. For example, if a user is assigned logon ID 1234 and password 567890, the next user is assigned logon ID 1235 and password 567891. Therefore, if an employee knows the ID of another person, the employee could easily determine the corresponding password and access the system using that person's ID.

Industry guidelines suggest management implement procedures to prevent unauthorized system access. Passwords should be changed at least every 60 days and, if they must be documented, the passwords should be secured from unauthorized access. These and other password policies are outlined in section 1-0250.00, Montana Operations Manual.

Department employees noted the CAMAS security software is not capable of automatically forcing a user to change the password. Therefore, the security officer must assign passwords to each user, and maintain a log of user ID and password assignments for reference.

To improve electronic access controls with the department's current access software, the security officer could periodically change passwords manually and the department could also evaluate software upgrades which may provide additional password security control. Unless password controls are improved, unauthorized individuals could access CAMAS and view or change confidential property valuation data.

Recommendation #8

We recommend the department implement procedures to require users change their CAMAS system passwords in compliance with state policy.

Electronic Access Should Agree with Employee Job Duties

Approximately 410 department employees have access to update property appraisal and valuation data within CAMAS. The department has established default access privileges for various employee job duties. The default privileges define recommended access levels for employees, depending on job duties. For example, access to the CAMAS security maintenance menu should be limited to employees with security officer or system administrator responsibilities. The department requires regional and county officials to notify the department in writing if an employee needs additional access beyond the default access initially granted.

Once granted, the access levels are not reviewed on a scheduled basis to determine if the access is appropriate based on the employee's current job duties. For instance, an employee may only require temporary access, or may change job duties. Unnecessary access privileges could allow employees to inappropriately change property characteristics such as square footage, construction grade,

number of bedrooms, etc., which in turn adjusts taxable values of the property.

The audit determined 11 employees are assigned the security access privilege. This allows the employees to add, change, and delete users, and gives the employees the ability to view other users' CAMAS passwords. Employees with security access privileges include a county assessor contracting with the state, an employee who has not worked for the department in over one year, and contract programmers assigned to maintain the system.

Industry guidelines suggest management implement controls to ensure user access agrees with employee job duties. Department employees indicated they were unaware of the access privileges assigned and noted they did not need the access provided to complete their job duties. The department believes employee responsibilities may have changed since the employees were first assigned access to CAMAS. Based on the testing performed, the department should confirm access granted with the employees' supervisor, periodically review access granted, and restrict employee access in accordance with job duties.

Recommendation #9

We recommend the department review employee access privileges to CAMAS on a scheduled basis and restrict access in accordance with job duties.

Changes to Employee-Owned Property Against Department Policy

Regional managers are requested to review employee-owned properties at least once every appraisal cycle, to ensure compliance with department policy. Department policy prohibits employees from appraising or making system changes to property they own, or property owned by family members.

During the audit we interviewed four regional managers who indicated they follow procedures to ensure employees do not appraise their own property. However, the procedures do not

prevent employees from adjusting CAMAS values or characteristics for employee-owned property.

We reviewed 54 department employees and identified 36 employees who own real property recorded on CAMAS. The audit determined 18 of the 36 employees entered changes to the properties they owned, based on our review of the CAMAS audit trail report. The audit trail reported changes to name and address, and property characteristic changes such as remodeling improvements, square footage, or condition. Changes to the property characteristics caused changes to the taxable valuation for some of the properties reviewed. Table 1 shows the types of changes made to the properties tested.

Table 1

Changes to Employee-Owned Property

#	Change Date	Name/Address change	Property Details	Valuation Change
1	9/92 8/93,9/94 1/96	•	• •	
2	11/90 9/92 3/93		• • •	
3	2/95	•		
4	8/92 12/95 3/95 4/96 8/96	•	• •	• •
5	2/92,11/92,6/93 10/93		•	•
6	5/92 7/92 5/93		• •	•
7	4/90,5/90,9/90 4/91	•	•	
8	10/91 5/92 6/92	•	• •	
9	2/93			•
10	5/92 10/94 5/95 10/95 1/96	• •	• •	•
11	11/92 1/93 12/93,7/95	•	• •	
12	12/92,2.95,5/95	•		
13	7/94,1/95,12/95,8/96	•		
14	1/91,11/91	•		
15	8/92 9/92 12/92 2/93 7/94 10/95 7/96		• • • • • • •	
16	4/95	•		
17	6/91 12/91 5/92 9/92 12/95			• • • • •
18	3/92		•	

=Sample Number (a single property owned by PAD employee).
Change Date= Date of Change (only changes made by owner/employee).
Name/Address Change=Street, mailing address, owner name,etc.
Property Details=Changes to property characteristics that are used in determining the valuation.
Valuation Change=Direct override of CAMAS valuation.

Source: Compiled by the Legislative Audit Division from department records.

Department management believe the employees used their own properties to test valuation changes because they are familiar with the property. We confirmed this to be true for many of the changes.

We believe the department should implement additional management controls to restrict employees from making changes to their properties on CAMAS. For example, the department could conduct an annual review of the CAMAS audit trail for properties owned by department employees, or limit system access privileges to prevent changes by employees. The department could also establish properties used specifically for test purposes or create a separate test area.

Recommendation #10

We recommend the department annually review employee-owned properties, and properties owned by their family members, to ensure compliance with department policy.

Internal Audit Follow-up Procedures Should be Established

The department's Property Assessment Division performs internal audits of CAMAS appraisal/assessment staff procedures. Internal audits address property valuation procedures and methodologies as implemented by employees according to department policy. The internal audit employees issue reports of their findings and recommendations to the counties, regions, and management staff. However, the department does not review the status of the audit recommendations to ensure the recommendations are implemented. Instead, the department requests county and regional staff implement the recommendations.

The audit reviewed the implementation status of recommendations at Blaine, Fergus, Gallatin, Madison, and Silver Bow counties. Prior internal audits had found a need to improve documentation for valuation decisions. However, regional supervisors at the counties were unable to provide evidence that they had implemented the department's recommendations. Without department follow-up, internal audit recommendations may not be implemented. We

believe the department should establish implementation deadlines and perform follow-up reviews to ensure the recommendations are implemented.

Department internal audit personnel indicated they are unable to conduct reviews at all county appraisal offices. The audit staff have directed their audit procedures to specific concerns, and complete the reviews in conjunction with previously scheduled office visits. Employees noted they may be unable to efficiently complete follow-up reviews on-site, based on their existing schedule. To save time and improve audit efficiency, the department could request county offices to report the implementation status for recommendations issued by the department. The department could also establish implementation deadlines and request county offices to report the status within the time frame.

Recommendation #11

We recommend the department establish procedures to ensure internal audit recommendations for CAMAS are implemented.

Chapter V - Department-wide Issues

Introduction

This chapter addresses audit issues common to RCS, DAR, IIT and CAMAS as discussed in Chapters II, III, and IV. Specific recommendations regarding electronic access controls within the CAMAS processing environment are included in Chapter IV. This chapter discusses electronic access controls specific to RCS, DAR, and IIT, which process data at the Department of Administration's mainframe data center.

In addition this chapter provides recommendations concerning disaster recovery procedures and security evaluations over information technology resources. We believe implementation of the recommendations included in this chapter and throughout the report will assist the department to improve overall general and application controls.

Electronic Access Issues - RCS, DAR and IIT

Electronic access privileges allow users to view, change, or delete application data. In addition to reviewing employee access to CAMAS, as discussed in Chapter IV, the audit reviewed employee access to RCS, DAR, and IIT by comparing assigned access privileges to employee job duties. The objective was to ensure access is restricted according to employee procedures and functions consistent with their job duties.

The audit identified employees have unnecessary update access to RCS, DAR and IIT application programs and/or data. Update access allows employees to add or change data included on income tax returns such as income, withholding, exemptions, and deductions. Update access also allows employees to correct processing errors identified by system edits or override the edit errors. Access to RCS and DAR could allow unauthorized changes to revenue collection data or outstanding tax receivable balances, respectively. The audit also found employee access was documented for some but not all employees, on authorized request forms.

Operations Division employees, responsible for programming and system support, have unlogged write access to application production programs and data. Write access allows users to change or update production programs and data without logging on to the

applications. Unlogged write access could allow the employees to alter production program processing functions or change application data without authorization by the division responsible for processing the data.

Programmer write access to production programs and data should be restricted, logged and monitored. Documented and properly authorized access requests help management maintain security over system data. Request forms could also document the employee's agreement to abide by the department's policy concerning access to confidential information.

The department should limit employee access to application data in accordance with job duties. Unnecessary access privileges compromise the integrity of data processed by the RCS, DAR, and IIT applications.

Recommendation #12

We recommend the department:

A.   **Restrict employee access to department-wide applications according to job duties.**

B.   **Document the access provided.**

Disaster Recovery Plans
Should be Completed

The department has not completed a formal disaster recovery plan to return department applications to normal operations following a disaster. An effective disaster recovery plan should allow management to restore computing operations in a set time and minimize losses.

Industry standards suggest management develop formal procedures to efficiently recover computer processing activities to normal operations following a disaster. The Montana Operations Manual section 1-0240.00 outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing information and resource requirements

necessary to maintain applications; and determining alternate procedures which may be necessary if recovery cannot be completed timely.

A disaster recovery plan may include but is not limited to:

► An inventory of current applications, operating system programs, telecommunications programs or networks, and hardware.

► An analysis to determine application significance and impact of loss, to define mission-critical applications which must be recovered.

► An analysis to determine application recovery priority.

► Selecting a disaster recovery method depending on how long the organization can operate without processing, management's backup procedures, and cost.

► Identification, involvement, and commitment of employees responsible for operating applications.

► Definition of application requirements including personnel, hardware, system support programs, communications, data, special forms, etc.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a complete disaster recovery plan which defines department responsibilities and requirements, the department may be unable to process its applications.

The department has tested recovery of its AS/400 data center and CAMAS application in conjunction with annual tests at the DofA hotsite facility. Although the DofA can recover agency applications and provide mainframe connection capabilities for agency-owned terminals, it cannot define agency application recovery priorities or personnel responsibilities. We encourage the department to continue working with the DofA to complete disaster recovery procedures for mission-critical applications.

<u>Recommendation #13</u>

We recommend the department document and test formal disaster recovery procedures for department mission-critical applications.

Internal Evaluations of Security

The issues identified during this audit indicate the department should establish procedures to evaluate information systems security in accordance with state law. Section 2-15-114, MCA, requires the department to be ". . . responsible for assuring an adequate level of security for all data and information technology resources within the department and shall. . . .(4) ensure internal evaluations of the security program for data and information technology resources are conducted." The department should implement policies which address safeguarding data and information technology resources. These policies should encourage the department to adopt procedures which include, but are not limited to, the following:

▸   Conduct and periodically update a comprehensive risk analysis to determine security threats to data and information resources.

▸   Develop and periodically update written policies and procedures which provide security over data and information resources.

▸   Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified risks to data and information resources.

▸   Perform periodic internal audits and evaluations of the security program for data and information resources.

The report findings address: income tax tolerance level and processing edit/error correction procedures; physical security controls over data center operations; electronic access controls over applications; operating system software controls; and disaster recovery contingency planning. The access control issues indicate the department should perform a thorough review of user access to

the department's applications, document access provided to users, and limit access according to employee job duties.

The audit determined the department does have policies to establish security procedures applicable to AS/400 data processing, but found the procedures have not been documented. Department-wide policies should be implemented to ensure data processing activities are controlled and completed according to management's expectations. A periodic review of internal security and procedures could improve overall general and application controls for the department's applications.

Recommendation #14

We recommend the department implement formal policies which address safeguarding information technology resources in accordance with state law.

Summary

Overall, the audit determined the RCS, DAR, IIT and CAMAS applications process data as intended. The issues address improving department procedures for processing data through the applications. For example, centralized case note documentation between IIT and DAR would improve account collection procedures. IIT issues address documenting system edits and tolerance levels and review of adjustments to tax returns. CAMAS issues address improving physical security within the data center and providing offsite storage for backup data. The department should also improve internal security of the CAMAS operating system, application passwords, and overall employee access controls.

The department is evaluating replacing the IIT, DAR and CAMAS systems with newer technology. Limitations within these systems have required the department implement alternative manual procedures to review and evaluate data processing results. For example, the CAMAS audit trail report is not useful for regular management review of changes employees make to property data. CAMAS also does not provide the ability to change user passwords.

IIT and DAR applications do not provide centralized case note data, which requires employees to maintain separate notes within each application. Our recommendations address improving system functionality, employee procedures, and application controls. The recommendations, if incorporated into existing or new systems, will improve the department's data processing procedures.

State of Montana

Marc Racicot, Governor

Department of Revenue

Mick Robinson, Director

P.O. Box 202701
Helena, Montana 59620-2701

November 26, 1996

Mr. Scott Seacat, Legislative Auditor
Legislative Audit Division
Room 135, State Capitol
P. O. Box 201705
Helena, Montana 59620-1705

NOV 2 6 1996

Dear Mr. Seacat:

The Department of Revenue responses to the 1996 EDP audit report recommendation are as follows:

Recommendation #1 We recommend the department evaluate system procedures to ensure IIT address changes do not over-write existing DAR address data.

Concur: We agree that on-line access to the "audit trail" of address changes would be an improvement, however, we would point out this historical information is still available within the department and can be researched, it is just not as readily accessed.

We believe the solution to this problem is to develop a "universal note screen" common to all systems within Revenue. Regrettably, we do not have adequate programming resources available to address this request nor have we had for some time. This is the case given the age and complexity of our existing systems, their requirement for extensive maintenance, and the Que of mission-critical work that continually displaces requests such as universal note screens.

The department is requesting funding from the 1997 Legislative Assembly to replace the existing department computer operating systems. Until the Legislature has acted on this request, no material new investment will be made in the existing systems. If the legislature does not approve the department's request, we will continue to carry this service request until we can identify available resources to develop the desired solution.

Recommendation #2. We recommend the department document Individual Income Tax system edits for management and personnel review.

Concur: We agree and will begin immediately to review and update documentation related to all IIT system edits.

Recommendation #3. We recommend the department establish procedures for periodic review of processing edit adjustments completed by Office Audit Bureau employees.

Concur: We agree this would be a desired system output. Unfortunately, even though the IIT system creates an electronic file of this activity, it is unavailable to management in any type of readable format due to lack of system programming. As explained in response to recommendation #1, division management has a long standing request to enhance the management reporting obtainable from the existing system. Again, the reason it has not yet been delivered relates to the systems' complexity, the maintenance requirements, and the Que of more critical needs to be addressed.

Until the Legislature provides direction on upgrading our present environment, we will not expend scarce programming resources to make further investment in the existing IIT system. If the legislature does not approve the department's requests, we will continue to carry this service request until we can identify available resources to develop the desired solution.

Recommendation #4 We recommend the department document and communicate its policy for adjusting tolerance errors and implement procedures to ensure compliance with the policy.

Concur: We agree that updated documentation and better internal communication will improve consistency in applying processing edits related to tolerance errors. We will take steps to accomplish both of these suggestions before we commence processing 1996 returns.

Recommendation #5 We recommend the department implement cost-effective controls to prevent or limit damage to computer facility equipment.

Concur: We agree and will take immediate steps to accomplish this recommendation.

Recommendation #6 We recommend the department ensure backup information is stored in a secure off-site location away from the computer facility.

Concur: We agree and will take immediate steps to accomplish this recommendation.

Recommendation #7 We recommend the department:

A. Evaluate and document AS/400 operating system installation parameters.

B. Develop security procedures over the AS/400 as required by department policy.

Concur: We agree and will take immediate steps to accomplish this recommendation

Recommendation #8 **We recommend the department implement procedures to require users change their CAMAS system passwords in compliance with state policy**.

Concur: Access to CAMAS is controlled through three levels of security. At the CAMAS level, the changes in the password methodology will require programming changes by our software vendor. We do not have an estimate of the cost required at this time. The department's budget is severely limited this year and this change may have to wait until resources are available for change.

Also, it is the intent of the department to request this feature to be built into the RFP for the integrated land assessment system which is being requested during the next biennium.

Recommendation #9 **We recommend the department review employee access privileges to CAMAS on a scheduled basis and restrict access in accordance with job duties**.

Concur: We agree and will take immediate steps to accomplish this recommendation.

Recommendation #10 **We recommend the department annually review employee-owned properties and properties owned by their family members, to ensure compliance with department policy.**

Concur: We agree and will take immediate steps to accomplish this recommendation.

Recommendation #11 **We recommend the department establish procedures to ensure internal audit recommendations for CAMAS are implemented.**

Concur: We agree and will take immediate steps to accomplish this recommendation.

Recommendation #12 **We recommend the department:**

A. Restrict employee access to department-wide applications according to job duties.

B. Document the access provided.

Concur: We agree and will take immediate steps to accomplish this recommendation

Recommendation #13 **We recommend the department document and test formal disaster recovery procedures for department mission-critical applications.**

Concur: We agree and will take immediate steps to accomplish this recommendation

Recommendation #14 **We recommend the department implement formal policies which address safeguarding information technology resources in accordance with state law.**

Concur: We agree and will take immediate steps to accomplish this recommendation

Thank you for your courtesy on the audit.

Sincerely,

Mick Robinson
Director